Red Hat Enterprise Linux for SAP Solutions 9

SAP HANA 実行ファイルのみを許可するように fapolicyd を設定する

Last Updated: 2024-05-02

Red Hat Enterprise Linux for SAP Solutions 9 SAP HANA 実行ファイルのみを許可するように fapolicyd を設定する

法律上の通知

概要

このポリシーを設定すると、SAP HANA を実行する環境がローカルおよびリモートの侵入、悪用、悪意のあるアクティビティーから保護されます。

目次

多様性を受け入れるオープンソースの強化

Red Hat では、コード、ドキュメントにおける配慮に欠ける用語の置き換えに取り組んでいます。まずは、マスター (master)、スレーブ (slave)、ブラックリスト (blacklist)、ホワイトリスト (whitelist) の 4 つの用語の置き換えから始めます。この取り組みは膨大な作業を要するため、今後の複数のリリースで段階的に用語の置き換えを実施して参ります。多様性を受け入れる用語に変更する取り組みの詳細は、Red Hat CTO である Chris Wright のメッセージ を参照してください。

RED HAT ドキュメントへのフィードバック (英語のみ)

Red Hat ドキュメントに関するご意見やご感想をお寄せください。また、改善点があればお知らせください。

Jira からのフィードバック送信 (アカウントが必要)

1. Jira の Web サイトにログインしていることを確認してください。
2. こちらのリンク をクリックして、フィードバックをお寄せください。
3. **Summary** フィールドにわかりやすいタイトルを入力します。
4. **Description** フィールドに、ドキュメントの改善に関するご意見を記入してください。ドキュメントの該当部分へのリンクも追加してください。
5. 今後の更新に関する通知を受け取りたい場合は、**Reporter** としてご自身が割り当てられていることを確認してください。
6. ダイアログの下部にある **Create** をクリックします。

第1章 FAPOLICYD の概要

fapolicyd ソフトウェアフレームワークは、ユーザー定義のポリシーに基づいてアプリケーションの実行を制御します。このフレームワークは、最適な方法で、システム上で信頼されていないアプリケーションや悪意のあるアプリケーションを実行されないようにします。詳細は、RHEL 9 の セキュリティー強化 ガイドの fapolicyd を使用したアプリケーションのブロックと許可 を参照してください。

注記

以下に説明する手順では、検出されたすべての SAP HANA 実行可能ファイルを **fapolicyd** 信頼ファイルに格納します。このファイルには、信頼されたファイルのすべての名前、サイズ、チェックサムが含まれます。SAP HANA バイナリーとシェルスクリプトは、**fapolicyd** 信頼ファイルに含まれている場合にのみ実行できます。したがって、**fapolicyd** 信頼ファイルに含まれていない SAP HANA バイナリーまたはシェルスクリプトを実行すると、データの破損や損失などの望ましくない影響が発生する可能性があります。すべての手順を慎重にテストし、最初に非実稼働システムで適切な検証を行う必要があります。

第2章 FAPOLICYD を使用して SAP HANA インストールを保護する

SAP HANA インストールを保護するには、次の手順を実行できます。

- **fapolicyd** パッケージをインストールする。
- 整合性チェックを **SHA-256** ハッシュに設定する。
- シェルスクリプトを保護するためにカスタム **fapolicyd** ルールを追加する。
- SAP HANA ファイルを信頼できるものとしてマークする。
- **fapolicyd** サービスを有効にする。

2.1. FAPOLICYD パッケージのインストール

手順

- **fapolicyd** パッケージをインストールします。

```
# dnf install fapolicyd
```

検証

- 次のコマンドを使用して、**fapolicyd** サービスがインストールされていても現在実行されていないことを確認します。

```
# systemctl status fapolicyd
● fapolicyd.service - File Access Policy Daemon
   Loaded: loaded (/usr/lib/systemd/system/fapolicyd.service; enabled; vendor preset:
disabled)
   Active: inactive (dead) since Fri 2024-04-19 14:59:52 CEST; 1s ago
...
Apr 19 14:59:51 host01 fapolicyd[337927]: shutting down...
Apr 19 14:59:51 host01 systemd[1]: Stopping File Access Policy Daemon...
Apr 19 14:59:52 host01 systemd[1]: fapolicyd.service: Succeeded.
Apr 19 14:59:52 host01 systemd[1]: Stopped File Access Policy Daemon.
```

2.2. 整合性チェックを SHA-256 ハッシュに設定する

デフォルトでは、**fapolicyd** は、アプリケーションの実行をブロックする必要があるかどうかを決定する際にファイル名を検証します。より高いレベルの保護のために、この設定を **SHA-256** に変更できます。

前提条件

- **fapolicyd** パッケージがシステムにインストールされている。

手順

1. 任意のテキストエディターで **/etc/fapolicyd/fapolicyd.conf** ファイルを開きます。以下に例を示します。

```
# vi /etc/fapolicyd/fapolicyd.conf
```

2. 整合性オプションを設定し、デフォルト値の **none** を **sha-256** に変更します。

```
integrity = sha-256
```

変更を有効にするには、**fapolicyd** サービスを再起動する必要があります。ただし、**fapolicyd** 設定にさらに変更を加える必要があるため、今すぐ **fapolicyd** を再起動しないでください。

検証

- 正しい入力内容を確認してください。

```
# fapolicyd-cli --check-config
Daemon config is OK
```

SAP HANA ベンチマークは RHEL 9.2 でテストされました。その際、最初は **fapolicyd** が無効になり、その後有効になり、**fapolicyd** のパフォーマンスへの影響が評価されました。テストを実行できるようにするために、**fapolicyd** 信頼ファイルに合計 19,184 個のエントリーが追加されました。テストの 99% でパフォーマンスへの影響は 5% 以下で、テストの大部分で 1 - 3% の速度低下が発生しました。

特定のワークロードではパフォーマンスの低下が大きくなる可能性があることに注意してください。したがって、潜在的な影響を正確に観察するには、特定の環境内でパフォーマンスを徹底的に評価する必要があります。

2.3. シェルスクリプトを保護するためのカスタム FAPOLICYD ルールの追加

デフォルトでは、**fapolicyd** はバイナリー実行可能ファイルと特定のプログラム (Python など) の実行をブロックします。SAP HANA インストールディレクトリー内のシェルスクリプトも保護するには、新しいカスタムルールを追加する必要があります。

前提条件

- **fapolicyd** パッケージがシステムにインストールされている。

手順

1. **/etc/fapolicyd/rules.d** ディレクトリーを開きます。
2. 71 で始まるファイル名を持つ新しいファイル (提案ファイル名: **71-sap-shellscript.rules**) を追加し、次の内容で、ルールがファイル **70-trusted-lang.rules** と **72-shell.rules** のルールの間に配置されます。

```
# Deny shell script execution and sourcing under SAP HANA directories

deny_audit perm=any all : ftype=text/x-shellscript dir=/hana/,/usr/sap/ trust=0
```

3. ファイルの所有権を **/etc/fapolicyd/rules.d** 内の他のファイルの所有権と同じに設定します。

```
# chown root:fapolicyd 71-sap-shellscript.rules
```

4. 次のコマンドを使用して、新しいルールが定義されていることを確認し、新しいルールをロードします。

```
# fagenrules --check
/usr/sbin/fagenrules: Rules have changed and should be updated
# fagenrules --load
```

検証

- ルールが更新されたことを確認します。

```
# fagenrules --check
/usr/sbin/fagenrules: No change
```

2.4. SAP HANA ファイルを信頼できるものとしてマークする

前提条件

- **fapolicyd** パッケージがシステムにインストールされている。

手順

1. まだインストールしていない場合は、SAP HANA ソフトウェアをインストールします。

2. 次のコマンドを使用して、すべての SAP HANA ファイルを **fapolicyd** 信頼データベースに追加します。**hana** や **usr_sap** など、ディレクトリーツリーごとに個別の信頼ファイルを使用することが推奨されます。

```
# fapolicyd-cli --file add /hana --trust-file hana
# fapolicyd-cli --file add /usr/sap --trust-file usr_sap
```

これにより、**/etc/fapolicyd/trust.d** ディレクトリーに **hana** と **usr_sap** という名前の 2 つのファイルが作成され、**/hana** と **/usr/sap** の下にあるすべてのファイルのエントリーが含まれます。

3. 新しくインストールされた RHEL システムに SAP HANA をインストールする場合は、SAP HANA インストーラーによって **/hana** および **/usr/sap** ディレクトリーが作成されるため、これらのディレクトリー内のすべてのファイルが有効な SAP ファイルであると信頼できます。
それ以外の場合、SAP HANA インストーラーによって作成されていないファイルがそれらのディレクトリーに存在する可能性があります。

   したがって、信頼ファイル **/etc/fapolicyd/trust.d/hana** および **/etc/fapolicyd/trust.d/usr_sap** 内のすべてのファイルが有効な SAP ファイルであることを慎重に確認する必要があります。考えられる方法の 1 つを以下に説明します。

   i. 新しくインストールされた別の RHEL システムに、新規の SAP HANA インストールを実行します。

   ii. そのシステムで手順 2 を繰り返します。

   iii. 両方のシステムの結果の信頼ファイルを比較します。

2.5. FAPOLICYD サービスの有効化

前提条件

- **fapolicyd** パッケージはインストールされているが、現在システム上で実行していない。
- これまでの手順をすべて完了している。

手順

- **fapolicyd** サービスを有効にして開始します。

```
# systemctl enable --now fapolicyd
```

fapolicyd サービスが SAP HANA システムを保護するようになりました。 **fapolicyd** 信頼ファイルに含まれていない **/hana** または **/usr/sap** 内のスクリプトとバイナリーはブロックされ、非 root ユーザーはこれらのファイルを実行できません。

検証

1. **fapolicyd** サービスが起動して実行していることを確認します。

```
# systemctl status fapolicyd
● fapolicyd.service - File Access Policy Daemon
    Loaded: loaded (/usr/lib/systemd/system/fapolicyd.service; enabled; preset: disabled)
    Active: active (running) since Thu 2024-03-14 16:38:32 IST; 18h ago
...
Mar 14 16:38:33 host01 fapolicyd[579216]: Trust database checks OK
Mar 14 16:38:33 host01 fapolicyd[579216]: Starting to listen for events
```

2. SAP HANA 管理者ユーザー (例: **h70adm**) を含む非 root ユーザーが、 **/hana** および **/usr/sap** 内の新しいスクリプトおよびバイナリープログラムを実行できないことを確認します。

```
# cp -pi /usr/bin/date /hana/
# su - h70adm
h70adm@host01:/usr/sap/H70/HDB35> /hana/date
-sh: /hana/date: Operation not permitted
h70adm@host01:/usr/sap/H70/HDB35> cat > try-to-start-me.sh
#!/bin/bash
echo "I will not execute."
<ctrl>d
h70adm@host01:/usr/sap/H70/HDB35> chmod u+x try-to-start-me.sh
h70adm@host01:/usr/sap/H70/HDB35> ./try-to-start-me.sh
-sh: ./try-to-start-me.sh: Operation not permitted
h70adm@host01:/usr/sap/H70/HDB35> rm try-to-start-me.sh
h70adm@host01:/usr/sap/H70/HDB35> exit
# rm /hana/date
rm: remove regular file '/hana/date'? y
```

第3章 SAP HANA の更新時に FAPOLICYD 信頼ファイルを再作成する

前提条件

- **fapolicyd** パッケージがシステムにインストールされている。
- SAP HANA ソフトウェアディレクトリーに新しい実行可能ファイルがないことを確認しました。これにより、不明なソースからのソフトウェアが誤って追加されることはありません。詳細は、SAP HANA ファイルを信頼できるものとしてマークする を参照してください。

手順

1. SAP HANA ソフトウェアの更新を実行する前に、**fapolicyd** を停止します。

```
# systemctl stop fapolicyd
```

2. 既存の **fapolicyd** 信頼ファイル **/etc/fapolicyd/trust.d/hana** および **/etc/fapolicyd/trust.d/usr_sap** のバックアップを作成し、これらのファイルを削除します。
3. SAP HANA ソフトウェアの更新を実行します。
4. SAP HANA ファイルを信頼済みとしてマークする 手順セクションのステップ 2 を繰り返して、SAP HANA の **fapolicyd** 信頼ファイルを再作成します。
5. **fapolicyd** を起動します。

```
# systemctl start fapolicyd
```

第4章 FAPOLICYD に関連する問題のトラブルシューティング

fapolicyd に関連する問題を診断するには、次の操作を実行します。

- **fapolicyd** アクセス統計については、**/var/log/fapolicyd-access.log** ファイルを確認してください。
- **fapolicyd** をデバッグモードで実行します。

fapolicyd 関連の問題の診断の詳細は、fapolicyd 関連の問題のトラブルシューティング を参照してください。

第5章 関連情報

- **fapolicyd** 信頼ファイルにさらにファイルを追加した後、次のコマンドを使用して **fapolicyd** データベースを更新します。

```
# fapolicyd-cli --update
```

- **fapolicyd** 信頼ファイルからエントリーを削除した後、代わりに **fapolicyd** を再起動する必要があります。

```
# systemctl restart fapolicyd
```